Notes on random reals*

Daniel Osherson
Princeton University

Scott Weinstein
University of Pennsylvania

September 14, 2012

The theory of random real numbers is exceedingly well-developed, and fascinating from many points of view. It is also quite challenging mathematically. The present notes are intended as no more than a gateway to the larger theory. They review just the most elementary part of the theory (bearing on Kolmogorov- and Martin-Löf-randomness). We hope that the simple arguments presented here will encourage the enterprising student to examine richer treatments of the subject available elsewhere, notably, in Downey and Hirschfeldt (2010).[1] Comments and corrections to the notes are, of course, welcome.

1 Notation and other preliminaries

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$. By a **sequence** we mean an infinite sequence ordered like $\mathbb{N}$. Given $n \in \mathbb{N}$ and infinite sequence x, we use $x(n)$ to denote the nth member of x, and $x[n]$ to denote the initial finite sequence of length n in x. So $x[0]$ is the empty sequence. An infinite sequence over $\{0, 1\}$ is called a **real**. Let B be the set of *finite* binary strings. The concatenation of $b, c \in \mathsf{B}$ is denoted $b \star c$. For $n \in \mathbb{N}$, 1^n denotes n 1's in a row. The length of $b \in \mathsf{B}$ is denoted $|b|$. For $b \in \mathsf{B}$ and infinite binary sequence x we write $b \subset x$, just in case there is an $n \in \mathbb{N}$ with $b = x[n]$. Similarly, for $a, b \in \mathsf{B}$ we write $b \subseteq a$, just in case b is an initial segment of a. For $b \in \mathsf{B}$, $O(b)$ denotes the set of reals that begin with b. For $B \subseteq \mathsf{B}$, $O(B) = \{O(b) : b \in B\}$. All uses of $\log$ are base 2.

*Contact: osherson@princeton.edu, weinstein@cis.upenn.edu.

[1] One small conceptual contribution to the theory is offered in Osherson and Weinstein (2008).

We fix an effective enumeration $\tau(m)$ of B, $m \in \mathbb{N}$. Members of B are enumerated according to length with ties broken lexicographically.

(1) LEMMA: For all $m \in \mathbb{N}$, $|\tau(m)| \leq \log(m+1)$.

(2) DEFINITION: Let $Q \subseteq \mathsf{B}$ be given. We say that Q is **closed under subsequences** just in case for all $b \in Q$, $a \in Q$ for every $a \subseteq b$.

For proof of the the following well-known result see Boolos, Burgess, and Jeffrey (2002, pp. 323-324).

(3) LEMMA: (König) Let $Q \subseteq \mathsf{B}$ be infinite and closed under subsequences. Then there is a real x such that $x[n] \in Q$ for all n.

We sometimes identify a real x (as understood here as an infinite sequence over $\{0,1\}$) with a real number in the interval $[0,1]$ via the map I that sends x to $\sum_{i=0}^{\infty} x(i) \cdot 2^{-(i+1)}$. Similarly, we may identify the finite initial segment $x[n]$ with the rational number $\sum_{i=0}^{n-1} x(i) \cdot 2^{-(i+1)}$. Any such finite sum yields a rational number called **dyadic**. Observe that I^{-1} is well-defined for all reals in $[0,1]$ aside from the positive dyadic rationals. Indeed, each dyadic rational besides 0 is the I image of exactly two infinite binary sequences. One of the sequences ends in a tail of 0's, the other in a tail of 1's. For example, the real number $\frac{1}{8}$ equals both $I(111000\cdots)$ and $I(110111\cdots)$. When mapping real numbers into real binary sequences, we must therefore choose between the two kinds of tails. The theory below can be developed on the basis of either choice. We prefer the latter.

(4) CONVENTION: For every positive, dyadic rational number r, we take its representation as a sequence over $\{0,1\}$ to end in an infinite sequence of 1's.

The convention resolves all ambiguity; every other real number has a unique inverse image under I.

It is tempting to introduce notation that distinguishes between "reals" in the sense of sequences over $\{0,1\}$ from "reals" in the sense of numbers (points on the real line). We bow to

custom, however, and rely on context to clarify whether "real" is used in one sense or the other. Note that whenever a statement involves an inequality (or weak inequality) then the map I is used implicitly. Similarly, when a real number x is juxtaposed with $[n]$ to form $x[n]$ then we have first implicitly applied I^{-1} to x to produce a sequence over $\{0,1\}$. The following lemma makes use of these conventions, and codifies a few well-known facts that we will refer to in later sections.

(5) LEMMA:

(a) $$\sum_{i=n+1}^{\infty} \left(\frac{1}{2}\right)^i = \left(\frac{1}{2}\right)^n.$$

(b) For all reals x and all $n \in \mathbb{N}$, $x[n] \leq x \leq x[n] + 2^{-n}$.

(c) For every real number $x \in (0,1]$, $x[n] < x$.

(d) For all $n \in \mathbb{N}$, $\sum_{i<n} 2^i = 2^n - 1$.

Proof: Fact (a) is an immediate consequence of the following well-known identity by setting $r = 1/2$.

For every real number $0 \leq r < 1$ and $n \in \mathbb{N}$, $\quad (1-r) \cdot \sum_{i=n}^{\infty} r^i = r^n.$

Fact (b) follows immediately from (a).

Fact (c) follows from Convention (4) concerning the identification of real numbers in $(0,1]$ with infinite binary sequences which are *not* eventually constantly 0.

Fact (d) is easily proved by induction. □

2 Kolmogorov complexity

Let W_i index the computably enumerable subsets of B (instead of indexing the computably enumerable subsets of N, which is more usual). The indexes on the W_i are qualified as "r.e." (recursively enumerable).

We use TM to abbreviate "Turing Machine." Members of B are conceived to be the inputs and outputs of TMs. Let M be a TM, and let $a, b \in \mathsf{B}$ be given. We write $M(a) = b$ just in

case M started with a on its tape halts with b on its tape. We write $\mathsf{TM}(b)\downarrow$ to signify that $\mathsf{TM}(b)$ is so defined, and $\mathsf{TM}(b)\uparrow$ to signify that it is undefined. Via a fixed, effective bijection between B and the set of TMs, TMs are themselves taken to be members of B. TMs thus inherit the ordering imposed above on B.

We write $\mathcal{C}_M(b)$ to be the length of a shortest $c \in \mathsf{B}$ such that $M(c) = b$; $\mathcal{C}_M(b) = \infty$ if no $c \in \mathsf{B}$ is such that $M(c) = b$; this number is known as the "plain Kolmogorov complexity" of b relative to M.

(6) DEFINITION: TM M is called **universal** just in case for every TM L there is $k \in \mathbb{N}$ such that $\mathcal{C}_M(b) \leq \mathcal{C}_L(b) + k$ for all $b \in \mathsf{B}$.

Note that the definition implies that $\mathcal{C}_M(b)$ is finite for every $b \in \mathsf{B}$ if M is universal. It's also worth observing that "universal" in the sense of Definition (6) does not yield the same set of machines as "universal" in Turing's original sense.

(7) LEMMA: Universal TMs exist.

Proof: Let A be a lexicographical ordering of all TMs. It follows immediately from the existence of universal machines in Turing's sense that there is a TM U such that for all $n \in \mathbb{N}$ and $d \in \mathsf{B}$, $U(1^n 0 d) = L(d)$, where $L = A(n)$. To verify that U is universal, let TM L be given, and let n be such that $L = A(n)$. Then for all $b \in \mathsf{B}$, $\mathcal{C}_U(b) \leq \mathcal{C}_L(b) + n + 1$. □

In light of the lemma, we fix a universal TM U, and we write $\mathcal{C}(b)$ in place of $\mathcal{C}_U(b)$. Let L be the TM that halts immediately, making no changes to its tape. Then for all $b \in \mathsf{B}$, $\mathcal{C}_L(b) = |b|$. Because U is universal there is $m \in \mathbb{N}$ such that $\mathcal{C}(b) \leq \mathcal{C}_L(b) + m$. It follows at once that:

(8) LEMMA: There is $m \in N$ such that for every $b \in \mathsf{B}$, $\mathcal{C}(b) \leq |b| + m$.

3 A fact about short instructions

An input to U can be conceived as instructions for producing an output. Inputs that are the shortest possible for producing their output are called *short*. Officially:

(9) DEFINITION: Call $p \in \mathsf{B}$ **short** if $U(p)\downarrow$, and for all $q \in \mathsf{B}$, if $U(p) = U(q)$ then $|p| \leq |q|$.

Equivalently:

(10) $p \in \mathsf{B}$ is short iff $\mathcal{C}(U(p)) = |p|$.

(11) PROPOSITION: There is no effective enumeration of an infinite number of short members of B.

Proof: We follow Li and Vitányi (1997, p. 121). For a contradiction, let p_i, $i \in \mathbb{N}$ be an enumeration of infinitely many short members of B. Then by (10), $\{\mathcal{C}(p_i) : i \in \mathbb{N}\}$ is unbounded. Therefore, the following function, $g : \mathsf{B} \to \mathsf{B}$, is total and computable.

For all $m \in \mathbb{N}$, $g(\tau(m)) = p_i$ where i is least such that $\mathcal{C}(p_i) \geq m$.

By the definition of g, we have:

(12) for all $m \in \mathbb{N}$, $\mathcal{C}(g(\tau(m))) \geq m$.

Suppose that TM L computes g. Then by the universality of the reference machine U there is $k \in \mathbb{N}$ such that:

(13) for all $m \in \mathbb{N}$, $\mathcal{C}(g(\tau(m))) \leq \mathcal{C}_L(g(\tau(m))) + k$.

Also, since the string $\tau(m)$ causes L to produce $g(\tau(m))$, and by Lemma (1):

(14) for all $m \in \mathbb{N}$, $\mathcal{C}_L(g(\tau(m))) \leq |\tau(m)| \leq \log(m+1) + 1$.

From (12) and (13):

(15) for all $m \in \mathbb{N}$, $m \leq \mathcal{C}_L(g(\tau(m))) + k$.

And from (14) and (15):

for all $m \in \mathbb{N}$, $m \leq \log(m+1) + k + 1$

which is false no matter which $k \in \mathbb{N}$ is chosen. □

4 Failure of a plausible account of randomness

A promising idea is to qualify real x as random just in case cofinitely many of x's initial segments have high complexity. In this section we specify this idea and show how it comes to grief.

(16) DEFINITION: Call $b \in \mathsf{B}$ **incompressible** just in case $\mathcal{C}(b) \geq |b|$.

Since there are 2^n binary strings of length n and only $\sum_{i<n} 2^i = 2^n - 1$ inputs to U of length less than n [see (5)d], it follows that:

(17) LEMMA: For every $n \in \mathbb{N}$ there are incompressible $b \in \mathsf{B}$ with $|b| = n$.

(18) DEFINITION: Call a real x **incompressible almost always** just in case

$$\{n : x[n] \text{ is incompressible}\}$$

is cofinite.

We might hope that the set of reals that are incompressible almost always is rich and numerous, but it turns out to be empty! We'll derive this surprising fact as a corollary to the following proposition.

(19) PROPOSITION: For all real x and all $k \in \mathbb{N}$ there is $n \in \mathbb{N}$ such that $\mathcal{C}(x[n]) < n - k$.

To prove the proposition, we start with a lemma.

(20) LEMMA: Let total recursive function $f : \mathsf{B} \to \mathsf{B}$ be given. Then there is $k \in \mathbb{N}$ such that for all $b \in \mathsf{B}$, $\mathcal{C}(f(b)) < \mathcal{C}(b) + k$.

Proof: Recall that U is our fixed universal TM, and let TM L be such that:

(21) for all $a \in \mathsf{B}$, $L(a) = f(U(a))$.

By Definition (6), let $k \in \mathbb{N}$ be such that:

(22) for all $c \in \mathsf{B}$, $\mathcal{C}(c) < \mathcal{C}_L(c) + k$.

Let $b \in \mathsf{B}$ be given, and let $a \in \mathsf{B}$ be of shortest length with $U(a) = b$. Hence:

(23) $\mathcal{C}(b) = |a|$.

By (21), $L(a) = f(b)$, hence:

(24) $\mathcal{C}_L(f(b)) \leq |a|$.

By (22) and (24), $\mathcal{C}(f(b)) < \mathcal{C}_L(f(b)) + k < |a| + k$, so by (23), $\mathcal{C}(f(b)) < \mathcal{C}(b) + k$. □

Proof of Proposition (19): Recall that $\tau(\cdot)$ is an effective bijection between $\mathbb{N}$ and B. Let effective $f : \mathsf{B} \to \mathsf{B}$ be such that for all $b \in \mathsf{B}$, $f(b) = \tau(|b|) \star b$. By Lemma (20) there is $k_0 \in \mathbb{N}$ such that for all $b \in \mathsf{B}$, $\mathcal{C}(f(b)) < \mathcal{C}(b) + k_0$. So by Lemma (8) there is $k_1 \in \mathbb{N}$ such that for all $b \in \mathsf{B}$, $\mathcal{C}(f(b)) < |b| + k_1$. Thus:

(25) for all $b \in \mathsf{B}$, $\mathcal{C}(\tau(|b|) \star b) < |b| + k_1$.

Now let real x and $k \in \mathbb{N}$ be given. To prove the proposition we must exhibit $n \in \mathbb{N}$ such that:

(26) $\mathcal{C}(x[n]) < n - k$.

Choose $p \in \mathbb{N}$ such that $\tau(p) \subset x$ and $|\tau(p)| > k_1 + k$. (That there is such a p is obvious.) Let $b \in \mathsf{B}$ be the p bits of x following $\tau(p)$, and let n be the length of $\tau(p) \star b$. Thus:

(27) (a) $|b| = p$

(b) $x[n] = \tau(p) \star b = \tau(|b|) \star b$

(c) $|h\tau(|b|)| = |\tau(p)| > k_1 + k$

(d) $|x[n]| = |\tau(|b|) \star b| = |\tau(p)| + |b| > k_1 + k + p$

By (27) and (25):

$$\mathcal{C}(x[n]) = \mathcal{C}(\tau(|b|) \star b) < |b| + k_1 = p + k_1 = (k_1 + k + p) - k < |x[n]| - k,$$

which verifies (26). □

(28) COROLLARY: No real is incompressible almost always.

Proof: Suppose for a contradiction that real x is incompressible almost always. Then

$$k = \sum \{i + \mathcal{C}(x[i]) : x[i] \text{ is not incompressible } \}$$

is well defined. It follows that for all $n \in \mathbb{N}$, $\mathcal{C}(x[n]) \geq n - k$, contradicting Proposition (19).

□

5 No subadditivity for $\mathcal{C}$

The following proposition is meant to deepen the conviction that $\mathcal{C}$ is not the right measure of complexity for finite sequences. (But we admit to not understanding why this feature of $\mathcal{C}$ is considered a defect.)

(29) PROPOSITION: For every $\ell \in N$, there are $a, b \in \mathsf{B}$ such that $C(a \star b) \geq C(a) + C(b) + \ell$.

To prove the proposition, we start with two lemmas.

(30) LEMMA: Let $P \subseteq \mathsf{B}$ and suppose that for all real x there is an $n \in \mathbb{N}$ such that $x[n] \in P$. Then, there is an $m \in \mathbb{N}$ such that for all real x there is an $n < m$ such that $x[n] \in P$.

Proof of Lemma (30): Suppose that

(31) for every $m \in \mathbb{N}$ there is an x such that for all $n < m$ $x[n] \notin P$.

Let $Q = \{a \in \mathsf{B} \mid \forall b(b \subseteq a \to b \notin P\}$. It follows from (31) that Q is infinite and closed under subsequences. Therefore, by Lemma (3) there is a real x such that for all $n \in N$ $x[n] \in Q$. Since $Q \subseteq \overline{P}$, this contradicts the hypothesis of (30). □

(32) DEFINITION: Call $b \in \mathsf{B}$ k-**compressible** just in case $\mathcal{C}(b) \leq |b| - k$.

(33) LEMMA: For every $k \in \mathbb{N}$, there is an $m \in \mathbb{N}$ such that for every $a \in \mathsf{B}$, if $|a| \geq m$, then there is $d \subset a$ such that d is k-compressible.

Proof: Fix k and let $P \subseteq \mathsf{B}$ be the collection of k-compressible sequences. Proposition (19) guarantees that for every real x there is an n such that $x[n] \in P$. The lemma now follows at once from Lemma (30). □

Proof of Proposition (29): Fix $\ell \in N$. By Lemma (8), choose m so that for every $b \in \mathsf{B}$, $\mathcal{C}(b) \leq |b| + m$. Let $k = \ell + m$. By Lemmas (17) and (33), we may choose an incompressible $a \in \mathsf{B}$ and $d \subset a$ with d k-compressible. Let b be such that $a = d \star b$. Then

$$\begin{aligned}\mathcal{C}(d \star b) = \mathcal{C}(a) \geq |a| = |d \star b| = |d| + |b| \geq \mathcal{C}(d) + k + |b| \\ \geq \mathcal{C}(d) + m + \ell + \mathcal{C}(b) - m = \mathcal{C}(d) + \mathcal{C}(b) + \ell.\end{aligned}$$

□

6 Prefix-free sets

The defects in plain Kolmogorov complexity lead to an approach based on "prefix-free" subsets of B.

(34) DEFINITION:

(a) $S \subseteq \mathsf{B}$ is **prefix-free** just in case for all $a, b \in S$, neither $a \subset b$ nor $b \subset a$.

(b) A TM L is **prefix-free** just in case *domain*(L) is prefix-free [that is, for all $b \in \mathsf{B}$ and $c \subset b$, $L(b)\!\downarrow$ implies $L(c)\!\uparrow$].

(35) EXAMPLE: $T = \{b \in \mathsf{B} :$ for some $n \in \mathbb{N}, b = 1^n \star 0 \star a$ with $|a| = n\}$ is prefix-free, infinite, and effectively enumerable.

(36) LEMMA: For every r.e. $S \subseteq \mathsf{B}$ there is an r.e. $T \subseteq \mathsf{B}$ such that

(a) $O(S) = O(T)$ and

(b) T is prefix-free.

Moreover, an index for T can be found uniformly effectively from an index for S.

Proof: Given a recursive enumeration $s_0, s_1, \ldots$ of S, T can be constructed by the following induction which effectively constructs a chain $T_0 \subseteq T_1 \subseteq \cdots \subseteq \mathsf{B}$ with $T = \cup_i T_i$. (If $S = \emptyset$ then the construction will deliver an index for $\emptyset$.) Basis: $T_0 = \{s_0\}$. Induction step: Suppose the induction has been completed through stage n. Let T_n be the subset of T already defined. If s_{n+1} is neither a suffix nor prefix of any $t \in T_n$ then $T_{n+1} = T_n \cup \{s_{n+1}\}$. If for some $t \in T_n$, s_{n+1} extends t then $T_{n+1} = T_n$. If for some $t \in T_n$, t extends s_{n+1} then $T_{n+1} = T_n \cup Z$ where Z is defined as follows. Let k be the length of the longest sequence in T_n. Let

$$Z = \{t \in \mathsf{B} : |t| = k, s_{n+1} \subset t \text{ and } \forall t' \in T_n, t' \not\subset t\}.$$

It is easy to see that the T constructed in this way satisfies the conditions of the lemma. □

The following lemma is proved in Li and Vitányi (1997, p. 74).

(37) LEMMA: (KRAFT) Let ℓ_i be a sequence of natural numbers. There is a prefix-free subset of B with this sequence as lengths of its members iff

$$\sum 2^{-\ell_i} \leq 1.$$

Here is an effective version, proved in Downey and Hirschfeldt (2010, Thm. 3.6.1, p. 125).

(38) LEMMA: Let ℓ_i be a recursive enumeration of lengths such that

$$\sum_i 2^{-\ell_i} \leq 1.$$

Then there is a recursive enumeration a_i of a prefix-free set such that $|a_i| = \ell_i$.

7 Prefix-free complexity

Given a prefix-free TM L and $b \in \mathsf{B}$, we let $\mathcal{K}_L(b)$ be the length of a shortest $a \in \mathsf{B}$ such that $L(a) = b$; in the absence of any such a $\mathcal{K}_L(b) = \infty$.

(39) DEFINITION: A TM V is **prefix-free universal** just in case V is prefix-free and for every prefix-free TM L there is a constant $k \in \mathbb{N}$ such that for all $b \in \mathsf{B}$, $\mathcal{K}_V(b) \leq \mathcal{K}_L(b) + k$.

(40) PROPOSITION: Prefix-free universal TMs exist.

Proof: It is easy to verify the existence of a uniform-effective procedure P operating on TMs such that for all machines M:

(a) $P(M)$ is prefix-free.

(b) $P(M)$ computes the same function as M, if M is prefix-free.

Recall from Section 1 our effective ordering L_i of the TMs. Let TM V be such $V(1^\ell \star 0 \star a) = P(L_\ell)(a)$ for all $\ell \in \mathbb{N}$ and be undefined for inputs of any other form. To see that V is prefix-free, suppose that $a, b \in \mathsf{B}$ were such that $a \subset b$ and both $V(a)\downarrow$ and $V(b)\downarrow$. Then for some $\ell \in \mathbb{N}$, a and b have the forms $1^\ell \star 0 \star c$ and $1^\ell \star 0 \star d$, respectively, with $c \subset d$. But then $P(L_\ell)(c)\downarrow$ and $P(L_\ell)(d)\downarrow$, contradicting the prefix-free nature of $P(L_\ell)$.

To finish the proof, let ℓ be the least index of prefix-free TM L. Then, for all $a, b \in \mathsf{B}$, $L(a) = b$ implies $V(1^\ell \star 0 \star a) = P(L_\ell)(a) = L(a) = b$. Hence, for all prefix-free TMs L with smallest index index ℓ, $\mathcal{K}_V(b) \leq \mathcal{K}_L(b) + \ell + 1$ for all $b \in \mathsf{B}$. □

In light of the proposition, we fix a universal prefix-free TM V, and we write $\mathcal{K}(b)$ in place of $\mathcal{K}_V(b)$. It is clear that for every $b \in \mathsf{B}$ there is a prefix-free TM L with $L(b) = b$. We infer immediately that:

(41) LEMMA: The range of V is B.

Hence, $\mathcal{K}(b)$ is defined for all $b \in \mathsf{B}$.

8 Short $\mathcal{K}$ programs

(42) DEFINITION: Call $p \in \mathsf{B}$ **prefix-free short** if $V(p)\downarrow$ and for all $q \in \mathsf{B}$, if $V(p) = V(q)$ then $|p| \leq |q|$.

(43) PROPOSITION: There is no effective enumeration of an infinite number of prefix-free short members of B.

Proof: The argument is parallel to that for Proposition (11). Let $T = \{1^n 0 : n \in \mathbb{N}\}$. Then T is prefix-free, infinite, and effectively enumerable by increasing length, say, as t_i. So:

(44) for all $m \in \mathbb{N}$, $|t_m| = m + 1$.

For a contradiction, let p_i, $i \in \mathbb{N}$ be an effective enumeration of infinitely many prefix-free short members of B. Of course, $\{\mathcal{K}(p_i) : i \in \mathbb{N}\}$ is unbounded. So the following function $\psi : T \to \mathsf{B}$ is computable.

(45) For all $m \in \mathbb{N}$, $\psi(t_m) = p_i$, where i is least such that $\mathcal{K}(p_i) \geq 2m$.

By the definition of ψ:

(46) for all $m \in \mathbb{N}$, $\mathcal{K}(\psi(t_m)) \geq 2m$.

Suppose that TM L computes ψ. Then $\mathit{domain}(L) = T$ is prefix-free, so by Definition (39) there is $k \in \mathbb{N}$ such that:

(47) for all $m \in \mathbb{N}$, $\mathcal{K}(\psi(t_m)) \leq \mathcal{K}_L(\psi(t_m)) + k$.

Also, since t_m causes L to produce $\psi(t_m)$, and by (44):

(48) for all $m \in \mathbb{N}$, $\mathcal{K}_L(\psi(t_m)) \leq |t_m| = m + 1$.

From (46) and (47):

(49) for all $m \in \mathbb{N}$, $2m \leq \mathcal{K}_L(\psi(t_m)) + k$.

And from (48) and (49):

for all $m \in \mathbb{N}$, $2m \leq m + 1 + k$,

which is false no matter which $k \in \mathbb{N}$ is chosen. □

9 Subadditivity for $\mathcal{K}$

In contrast to Proposition (29), we have:

(50) PROPOSITION: There is $k \in N$ such that for all $a, b \in \mathsf{B}$, $\mathcal{K}(a \star b) \leq \mathcal{K}(a) + \mathcal{K}(b) + k$.

As a preliminary to the proof, let $a, b, c, d, e \in \mathsf{B}$ be such that $b = a \star c$ and $b = d \star e$ with $a \neq d$ (hence, $c \neq e$). Then no prefix-free TM can be defined on both a and d because one is a subsequence of the other. Since V is prefix-free, we thus have:

(51) LEMMA: For all $b \in \mathsf{B}$ there is at most one pair $a, c \in \mathsf{B}$ such that $b = a \star c$, $V(a)\downarrow$ and $V(c)\downarrow$. Moreover, if such a pair a, c exists, it can be found effectively (via dovetailing).

Proof of Proposition (50): By Lemma (51) let TM L be such that for all $b \in \mathsf{B}$, $L(b) = V(a) \star V(c)$ for the unique $a, c \in \mathsf{B}$ such that $b = a \star c$, $V(a)\downarrow$, and $V(c)\downarrow$; if no such a, c exist then $L(b)\uparrow$. To show that L is prefix-free, suppose that $b, b' \in \mathsf{B}$ were such that $b' \subset b$, $L(b)\downarrow$, and $L(b')\downarrow$. Then there are a, c and a', c' such that $b = a \star c$, $V(a)\downarrow$, $V(c)\downarrow$, $b' = a' \star c'$, $V(a')\downarrow$, $V(c')\downarrow$, and either $a \subset a'$, $a' \subset a$, $c \subset c'$ or $c' \subset c$. But this implies that V is not prefix-free, contradiction. Since L is prefix-free, by Definition (39) let $k \in \mathbb{N}$ be such that:

(52) for all $c \in \mathsf{B}$, $\mathcal{K}(c) \leq \mathcal{K}_L(c) + k$.

Now let $a, b \in \mathsf{B}$ be given. Let $p, q \in \mathsf{B}$ have shortest lengths such that $V(p) = a$ and $V(q) = b$, respectively. [That such p, q exist follows from Lemma (41).] Then by the definition of L,

(53) $L(p \star q) = V(p) \star V(q) = a \star b$.

By (52), $\mathcal{K}(a \star b) \leq \mathcal{K}_L(a \star b) + k$. By (53), $\mathcal{K}_L(a \star b) + k \leq |p \star q| + k = |p| + |q| + k$. And by the choice of p, q, $|p| + |q| + k = \mathcal{K}(a) + \mathcal{K}(b) + k$. Therefore, $\mathcal{K}(a \star b) \leq \mathcal{K}(a) + \mathcal{K}(b) + k$. □

10 Chaitin's halting probability

Recall that V is our reference prefix-free universal TM. We define the **halting probability**, Ω, as follows.

(54) DEFINITION:

$$\Omega = \sum \left\{ 2^{-|b|} : b \in \mathsf{B} \text{ and } V(b)\downarrow \right\}.$$

By Lemma (41), $\Omega > 0$ since $\{b \in \mathsf{B} : V(b)\downarrow\} \neq \emptyset$. On the other hand, by Lemma (37), $\Omega \leq 1$ inasmuch as *domain*(V) is prefix-free. So Ω may be conceived as a probability, namely, as the chance of hitting a sequence in *domain*(V) by flipping a fair coin. Note that the numerical value of Ω depends on the choice V of reference universal Turing Machine.

Define $P_n = \{b \in \mathsf{B} : |b| \leq n \text{ and } V(b)\downarrow\}$. Of course, for all $n \in \mathbb{N}$, P_n is finite. Following the development in Li and Vitányi (1997, p. 217) (but with some modifications), we now establish:

(55) LEMMA: There is a computable function ψ from B to finite subsets of B such that for all $n \in \mathbb{N}$, $\psi(\Omega[n]) = P_n$.

Proof: First we demonstrate:

(56) Let $X \subseteq$ *domain*(V) and suppose that $\sum\{2^{-|b|} : b \in X\} > \Omega[n]$. Then $P_n \subseteq X$.

For a contradiction, suppose that $P_n \not\subseteq X$. Then, for some $b \in \mathit{domain}(V)$ with $|b| \leq n$, $b \notin X$. Since $X \subseteq \mathit{domain}(V)$ it follows that:

(57) $\sum\{2^{-|b|} : b \in X\} \leq \Omega - 2^{-n}$.

But by (5)(b), $\Omega - 2^{-n} \leq \Omega[n]$, which with (57) contradicts the assumption $\sum\{2^{-|b|} : b \in X\} > \Omega[n]$, proving (56).

It was noted above that $\Omega > 0$ [indeed, Lemma (41) implies that $\mathit{domain}(V)$ is infinite]. Therefore, by (5)(c) for every $n \in \mathbb{N}$, $\Omega > \Omega[n]$. It follows at once that:

(58) For every $n \in \mathbb{N}$ there is a finite subset X of $\mathit{domain}(V)$ such that $\sum\{2^{-|b|} : b \in X\} > \Omega[n]$.

Now let us describe how to compute ψ. Given $a \in \mathsf{B}$, use dovetailing to enumerate $\mathit{domain}(V)$. Let $X \subseteq \mathit{domain}(V)$ be the first finite subset that emerges from the enumeration with the property that $\sum\{2^{-|b|} : b \in X\} > a$. [If no such X is found then $\psi(a)\uparrow$.] Set $\psi(a) = \{b \in X : |b| \leq |a|\}$.

Let $n \in \mathbb{N}$ be given. To finish the proof of Lemma (55), we show that $\psi(\Omega[n]) = P_n$. By (58), the enumeration of $\mathit{domain}(V)$ yields a finite subset X such that $\sum\{2^{-|b|} : b \in X\} > \Omega[n]$. By (56), $P_n \subseteq X$. Since P_n contains the members of $\mathit{domain}(V)$ with length bounded by n, $\psi(\Omega[n]) = \{b \in X : |b| \leq |\Omega[n]|\} = \{b \in X : |b| \leq n\} = P_n$. □

(59) COROLLARY: Ω is not computable. That is, the function mapping $n \in \mathbb{N}$ to $\Omega(n)$ is not effective.

Proof: Suppose for a contradiction that Ω is computable. Then Lemma (55) implies that P_n is computable from n. The set $P = \{p \in \mathsf{B} : V(p)\downarrow\}$ is therefore decidable. (Given $b \in \mathsf{B}$, $b \in P$ iff $b \in P_{|b|}$.) We may therefore enumerate P in order of increasing length. Thus, we can effectively enumerate the set S of $p_j \in P$ such that for no $i < j$, $V(p_i) = V(p_j)$. Each such p_j is prefix-free short in the sense of Definition (42). Since $\mathit{range}(V)$ is infinite, it is clear that S is infinite. Such an enumeration is impossible by Proposition (43). □

Since all rational reals are computable, we also have:

(60) COROLLARY: Ω is irrational. In particular, $\Omega < 1$.

Now we show the pivotal fact:

(61) PROPOSITION: There is a constant k such that for all $n \in N$, $\mathcal{K}(\Omega[n]) > n - k$.

Proof: From Lemma (55) it follows that there is computable $\varphi : \mathsf{B} \to \mathsf{B}$ such that for all $n \in \mathbb{N}$, $\varphi(\Omega[n]) \in \mathit{range}(V)$, and for all $b \in \mathsf{B}$, $\varphi(\Omega[n]) = V(b) \Rightarrow |b| > n$. Informally, φ is computed as follows. Given $\Omega[n]$, compute P_n then compute $X = \{V(b) : b \in P_n\}$. Enumerate the range of V until the first $a \in \mathsf{B}$ appears that is not in X. Set $\varphi(\Omega[n]) = a$. Hence:

(62) For all $n \in N$, $\mathcal{K}(\varphi(\Omega[n])) > n$.

Let TM L be such that for all $b \in \mathsf{B}$, $L(b) = \varphi(V(b))$ with $L(b)\uparrow$ if $V(b)\uparrow$. Then L is prefix-free because V is. Note that if $V(b) = \Omega[n]$ then $L(b) = \varphi(\Omega[n])$. It follows that:

(63) For all $n \in \mathbb{N}$, $\mathcal{K}_L(\varphi(\Omega[n])) \leq \mathcal{K}(\Omega[n])$.

Since L is prefix-free, by Definition (39), let $k \in \mathbb{N}$ be such that:

(64) For all $n \in \mathbb{N}$, $\mathcal{K}(\varphi(\Omega[n])) \leq \mathcal{K}_L(\varphi(\Omega[n])) + k$.

It follows at once from (63) and (64) that:

(65) For all $n \in \mathbb{N}$, $\mathcal{K}(\varphi(\Omega[n])) \leq \mathcal{K}(\Omega[n]) + k$.

From (62) and (65) we obtain

For all $n \in \mathbb{N}$, $n < \mathcal{K}(\Omega[n]) + k$.

which implies Proposition (61). □

(66) DEFINITION: Any real x for which there is a constant k such that for all $n \in N$, $\mathcal{K}(x[n]) \geq n - k$ is called **random in the sense of Kolmogorov**.

Proposition (61) thus shows:

(67) COROLLARY: There are reals that are random in the sense of Kolmogorov.

Later we'll see that the set of such reals has measure 1.

Notice that Definition (39) implies that the class of reals that are random in the sense of Kolmogorov is invariant under different choices of prefix-free universal TM.

11 Martin-Löf tests in sense 1

With minor differences, we start by following (Li and Vitányi, 1997, p. 141ff.). All probabilities in what follows are with respect to the uniform product measure (i.e., the coin flip measure). Given $S \subseteq \mathsf{B}$, let $O(S)$ be the set of reals that start with some $\sigma \in S$. To reduce clutter, we rely on the following convention.

(68) CONVENTION: Given $S \subseteq \mathsf{B}$, we write *Pr*(S) for *Pr*$(O(S))$.

The following lemma reflects the fact that members of a prefix-free subset of B dominate non-intersecting neighborhoods of the Cantor Space.

(69) LEMMA: Let $X \subseteq \mathsf{B}$ be prefix-free. Then *Pr*$(X) = \sum_{b \in X} 2^{-|b|}$.

For a function f, we write $f(x) \downarrow = y$ to mean that $f(x)$ is defined and equals y (and similarly for inequalities).

(70) DEFINITION: Any partial recursive function $t : \mathsf{B} \to N$ is called a **Martin-Löf test (in sense 1)** provided that for all $m \in N$,

$$Pr\{b \in \mathsf{B} : t(b)\downarrow \geq m\} \leq 2^{-m}.$$

(71) EXAMPLE: Let $t : \mathsf{B} \to N$ count the length of the initial sequence of 0's in a given $x \in \mathsf{B}$. Then t is a Martin-Löf test because for each $m \in N$, the set of reals that begin with at least m 0's has probability 2^{-m}. (For example, the probability of a real beginning with three 0's is $1/8$.)

To clarify notation, let us expand the foregoing example. Given $m \in \mathbb{N}$, $S = \{b \in \mathsf{B} : t(b)\downarrow \geq m\}$ is a subset of B. To calculate the probability of S, we consider the set of reals x that extend some member of S, that is, we consider the set $O(S)$. The relevant condition is therefore that $Pr(O(S)) \leq 2^{-m}$. Relying on Convention (68), the latter inequality is written as $Pr(S) \leq 2^{-m}$.

(72) EXAMPLE: Let $t : \mathsf{B} \to N$ count the number of consecutive even positions in a given $b \in \mathsf{B}$ that are filled with 1's starting from position 0. For $m = 3$, the probability of a real beginning with 1_1_1 is $1/8$, and more generally, the probability of beginning with at least m 1's in even position is 2^{-m}. So t is a Martin-Löf test.

(73) EXAMPLE: Let $t : \mathsf{B} \to N$ count the number of times 101 appears in a given binary sequence. Then t is *not* a Martin-Löf test. Indeed, for $m = 3$, the probability of a real containing at least m occurrences of 101 is unity (which exceeds $1/8$).

(74) EXAMPLE: Let $t : \mathsf{B} \to N$ count the number of consecutive 0's just after the initial segment 111 if it occurs. Then t is a Martin-Löf test even though t is partial. For each $m \in N$, the set of reals that begin with at least m 0's following the initial sequence 111 has probability 2^{-m+3}.

Since t can be *any* partial recursive function, the collection of Martin-Löf tests captures all sufficiently rare patterns that can be mechanically detected in binary sequences. The idea of "sufficient rareness" is given by the condition

$$Pr\{b \in \mathsf{B} : t(b)\downarrow \geq m\} \leq 2^{-m}$$

in Definition (70).

(75) DEFINITION: Let a Martin-Löf test t and a real x be given. We say that x **passes** t if $\{t(x[n]) : n \in N \text{ and } t(x[n])\downarrow\}$ is bounded. Otherwise, x **fails** t.

The idea is that x passes t if x doesn't manifest ever more improbable events according to t (namely, with probabilities declining as 2^{-m}).

(76) EXAMPLE: Let t be as in Example (72). Then a real x passes t if and only if $x(2n) = 0$ for some $n \in \mathbb{N}$.

(77) DEFINITION: A real x is **Martin-Löf random (in sense 1)** just in case x passes every Martin-Löf test (in sense 1).

12 Martin-Löf tests in sense 2

(78) DEFINITION: Let function $f : N \to N$ be total recursive. Then f is a **Martin-Löf test (in sense 2)** provided that for all $n \in N$, $Pr(W_{f(n)}) \leq 2^{-n}$.

(79) DEFINITION: Let f be a Martin-Löf test in sense 2. A real x **passes** f just in case $x \notin \bigcap\{O(W_{f(n)}) : n \in \mathbb{N}\}$, and x **fails** f otherwise). We call x **Martin-Löf random (in sense 2)** if x passes all Martin-Löf tests (in sense 2).

(80) PROPOSITION: If a real is Martin-Löf random in sense 2 then it is Martin-Löf random in sense 1.

Proof: Suppose that real x fails Martin-Löf test t in sense 1 [Definition (70)]. We must exhibit a Martin-Löf test f in sense 2 [Definition (78)] that x fails.

Let total recursive $f : N \to N$ be such that $f(0)$ is an r.e. index for B, and for all $n > 0$,

$$W_{f(n)} = \bigcup\{t^{-1}(m) : m > n\}.$$

Because t is partial recursive, it is clear that such an f exists. To see that f is a Martin-Löf test in sense 2, suppose for a contradiction that for some $n > 0$, $Pr(W_{f(n)}) > 2^{-n}$. Then $Pr(\bigcup\{t^{-1}(m) : m > n\}) > 2^{-n}$, hence:

(81) $$Pr\{b \in \mathsf{B} : t(b)\!\downarrow > n\} > 2^{-n}.$$

But (81) contradicts the assumption that t is a Martin-Löf test in sense 1 [Definition (70)]. To show that x fails f, suppose otherwise. Since $x \in O(\mathsf{B}) = O(W_{f(0)})$, there is $n > 0$ with

$$x \notin O(W_{f(n)}) = O(\bigcup\{t^{-1}(m) : m > n\}) = O(\{b \in \mathsf{B} : t(b)\!\downarrow \geq n + 1\}).$$

But $x \notin O(\{b \in \mathsf{B} : t(b)\downarrow \geq n+1\})$ implies that $\{t(x[n]) : n \in N \text{ and } t(x[n])\downarrow\}$ is bounded, which contradicts the assumption that x fails t [Definition (75)]. □

(82) PROPOSITION: If a real is Martin-Löf random in sense 1 then it is Martin-Löf random in sense 2.

Proof: Suppose that real x is not Martin-Löf random in sense 2. We will show that x is not Martin-Löf random in sense 1. Since x is not Martin-Löf random in sense 2 there is total recursive $g : \mathbb{N} \to \mathbb{N}$ such that:

(a) for all $n \in \mathbb{N}$, $Pr(W_{g(n)}) \leq 2^{-n}$

(b) $x \in \bigcap\{O(W_{g(n)} : n \in \mathbb{N})$.

Let total recursive $f : \mathbb{N} \to \mathbb{N}$ be such that $f(n) = g(n+1)$. Then:

(83) (a) for all $n \in \mathbb{N}$, $Pr(W_{f(n)}) \leq 2^{-(n+1)}$

(b) $x \in \bigcap\{O(W_{f(n)} : n \in \mathbb{N})$

Define (possibly partial) recursive function $t : \mathsf{B} \to \mathbb{N}$ such that for all $b \in \mathsf{B}$, $t(b) = |b|$ iff $b \in W_{f(|b|)}$, with $t(b)\uparrow$ if $b \notin W_{f(|b|)}$. To see that t is a Martin-Löf test in sense 1, let $m \in \mathbb{N}$ be given. Let $Z = \{b \in \mathsf{B} : t(b)\downarrow \geq m\}$. Then $Z = \{b \in \mathsf{B} : |b| \geq m \wedge b \in W_{f(|b|)}\} \subseteq W_{f(m)} \cup W_{f(m+1)} \ldots$. So by (83)a and Lemma (5)a,

$$Pr(Z) \leq \sum_{i=m+1}^{\infty} \left(\frac{1}{2}\right)^i = \left(\frac{1}{2}\right)^m$$

which exhbits t as a Martin-Löf test in sense 1. By (83)b, $\{t(x[n]) : n \in N \text{ and } t(x[n])\downarrow\}$ is unbounded, hence x fails t by Definition (75). □

(84) COROLLARY: A real is Martin-Löf random in sense 1 if and only if it is Martin-Löf random in sense 2.

Henceforth we proceed in sense 2. That is:

(85) CONVENTION: By a **test** is henceforth meant a Martin-Löf test in sense 2 [as described in Definition (78)]. Likewise, a real is called **Martin-Löf random** iff it is Martin-Löf random in sense 2.

13 Universal tests

(86) DEFINITION: A test f is *universal* just in case for all reals x, if x fails any test then x fails f.

(87) THEOREM: There is a universal test.

To prove the theorem, call tests f and g *congruent* iff for all $n \in \mathbb{N}$, $W_{f(n)} = W_{g(n)}$. Congruent tests may not be identical since they might exploit different indices for the same recursively enumerable set. Plainly:

(88) LEMMA: Tests congruent to each other are failed by the same set of reals.

Let φ_i be the usual indexing of partial recursive functions.

(89) LEMMA: There is total recursive $h : \mathbb{N} \to \mathbb{N}$ such that for all $i \in \mathbb{N}$:

(a) for all $n \in \mathbb{N}$, if $\varphi_{h(i)}(n)\!\downarrow$ then $Pr(W_{\varphi_{h(i)}(n)}) \leq 2^{-n}$; and

(b) if φ_i is a test then $\varphi_{h(i)}$ is a test that is congruent to φ_i.

Proof of Lemma (89): Informally, here is how to compute h. Let i be given. Then $h(i)$ is an effectively constructed index for the TM L that behaves as follows. Given $n \in N$, L computes $\varphi_i(n)$. If $\varphi_i(n) \uparrow$ then $L(n) \uparrow$. Otherwise, suppose that $\varphi_i(n) = m$. Then L constructs an index for the longest initial segment of the canonical enumeration of W_m whose sum of probabilities remains bounded by 2^{-n}. Therefore, $Pr(W_{\varphi_{h(i)}(n)}) \leq 2^{-n}$. Now suppose that φ_i is a test and let $n \in \mathbb{N}$ be given. Then $\varphi_i(n)\!\downarrow$ so $L(n)\!\downarrow$. Moreover, $Pr(W_{\varphi_i(n)}) \leq 2^{-n}$ so $W_{\varphi_{h(i)}(n)} = W_{\varphi_i(n)}$. Hence $\varphi_{h(i)}$ is a test, and congruent to φ_i. □

Proof of Theorem (87): Let h be as described in Lemma (89). Given $i, n \in N$, define $X(i,n)$ to be $W_{\varphi_{h(i)}(i+n)}$ if this set is defined, $= \emptyset$ otherwise. By Lemma (89)a, $Pr(X(i,n)) \leq 2^{-(i+n)}$. Hence:

(90) For all $n \in N$, $Pr \bigcup \{X(i,n) : i \in N\} \leq \sum_{i=1}^{\infty} 2^{-n-i} = 2^{-n} \sum_{i=1}^{\infty} 2^{-i} = 2^{-n}$.

A universal test f may now be defined as follows. Given $n \in \mathbb{N}$, f dovetails the enumerations of $W_{\varphi_{h(i)}(i+n)}$, $i \in \mathbb{N}$, to uniformly effectively construct an r.e. index $f(n)$ for $\bigcup \{X(i,n) : i \in N\}$. Thus:

(91) For all $n \in \mathbb{N}$, $W_{f(n)} = \bigcup \{X(i,n) : i \in N\}$.

By (90), f is a test. To see that f is universal, suppose that real x fails test g. We must show that x fails f. By Lemma (89)b, let $i \in N$ be such that g is congruent with $\varphi_{h(i)}$. By Lemma (88), x fails $h(i)$, that is:

(92) $x \in \bigcap \{O(W_{\varphi_{h(i)}(n)}) : n \in \mathbb{N}\}$.

To show that $x \in \bigcap \{O(W_{f(n)}) : n \in \mathbb{N}\}$, and thus complete the proof, it suffices to show that $x \in O(W_{f(n)})$ for given $n \in \mathbb{N}$. But by (92), $x \in O(W_{\varphi_{h(i)}(i+n)})$. So $x \in O(X(i,n)) \subseteq O(\bigcup \{X(i,n) : i \in N\}) = O(W_{f(n)})$ by (91). □

(93) COROLLARY: The probability of the set of Martin-Löf random reals is 1.

To prove the corollary, we rely on two lemmas the first of which may be found in (Oxtoby, 1971, Thm. 3.17).

(94) LEMMA: Suppose that A_i is a descending $\supseteq$-chain of measurable sets of reals. Then

$$Pr(\bigcap_i A_i) = \lim_{i \to \infty} Pr(A_i).$$

(95) LEMMA: For every test f there is a test g such that

(a) for all $i \in \mathbb{N}$, $W_{g(i)} \supseteq W_{g(i+1)}$, and

(b) a real fails g if and only it fails f.

Moreover, an index for g can be found uniform effectively from an index for f.

Proof: It suffices to let $g(n)$ be an index for $W_{f(0)} \cap \cdots \cap W_{f(n)}$. □

Proof of Corollary (93): For all $i \in \mathbb{N}$, $O(W_i)$ is measurable since it is the union of basic open sets [namely, $\bigcup\{O(b) : b \in W_i\}$]. By Theorem (87) and Lemma (95), let g be a universal test such that $\{W_{g(n)} : n \in \mathbb{N}\}$ forms a $\supseteq$-descending chain. By Definition (86), real x is Martin-Löf-random iff x passes g. By Definition (79), the set of reals that fail g is $\bigcap\{O(W_{g(n)}) : n \in \mathbb{N}\}$, whose probability is $\lim_{i\to\infty}$ *Pr*$(O(W_{g(n)}))$ by Lemma (94). By Definition (78), the latter limit is zero. Hence, the set of reals that pass g has probability 1. □

14 Equivalence of the two conceptions of randomness

It will be shown in this section that a real is random in the sense of Kolmogorov [Definition (66)] iff it is random in the sense of Martin-Löf [Definition (79)]. We abbreviate the two senses of randomness to "KC" and "ML" (The "C" in "KC" stands for "Chaitin").

(96) PROPOSITION: If a real is ML-random then it is KC-random.

The proof follows Downey and Hirschfeldt (2010, §6.2). We start with a lemma.

(97) LEMMA: Let TM M have prefix-free domain. Fix $k \in \mathbb{N}$, and let $S = \{b \in \mathsf{B} : \mathcal{K}_M(b) \leq |b| - k\}$. Then *Pr*$(S) \leq 2^{-k}$*Pr*(*domain*$(M)$).

Proof: For each $b \in S$ let $c_b \in \mathsf{B}$ be such that $|c_b| \leq |b| - k$ and $M(c_b) = b$. Then:

$$\begin{aligned}
\textit{Pr}(S) &\leq \sum\{2^{-|b|} : b \in S\} \\
&\leq \sum\{2^{-(|c_b|+k)} : b \in S\} \\
&= 2^{-k}\sum\{2^{-|c_b|} : b \in S\} \\
&\leq 2^{-k}\sum\{2^{-|d|} : d \in \textit{domain}(M)\} \\
&= 2^{-k}\textit{Pr}(\textit{domain}\, M).
\end{aligned}$$

The first inequality follows from Lemma (37) because S is a subset of the prefix-free set $\mathit{domain}(M)$. The second inequality comes from the choice of c_b. The third inequality follows from $c_b \in \mathit{domain} M$. The last equality relies on Lemma (69). □

Proof of Proposition (96): Let total recursive $f : \mathbb{N} \to \mathbb{N}$ be such that for all $k \in \mathbb{N}$, $W_{f(k)} = \{b \in \mathsf{B} : \mathcal{K}(b) \leq |b| - k\}$. A dovetailing construction shows that such an f exists. By Lemma (97), for all $k \in \mathbb{N}$, $\mathit{Pr}(W_{f(k)}) \leq 2^{-k} \mathit{Pr}(\mathit{domain}(W_{f(k)}))$. Since $\mathit{domain}(W_{f(k)}) \subseteq \mathit{domain}(V)$, and the latter set is prefix-free, we have by Lemma (69) that $\mathit{Pr}(\mathit{domain}(W_{f(k)}) \leq 1$. Hence, for all $k \in \mathbb{N}$, $\mathit{Pr}(W_{f(k)}) \leq 2^{-k}$ which exhibits f as a Martin-Löf test. Now suppose that real x is ML-random. Then for some $k \in \mathbb{N}$, $x \notin O(W_{f(k)})$. Hence, for all $m \in \mathbb{N}$, $\mathcal{K}(x[m]) \geq |b| - k$ so x is KC-random by Definition (66). □

Here is the converse to Proposition (96):

(98) PROPOSITION: If a real is KC-random then it is ML-random.

Proof: We prove the contrapositive. Suppose that real x is not ML-random. Then there is total recursive $f : N \to N$ such that $x \in \bigcap_n W_{f(n)}$ and $\mathit{Pr}(W_{f(n)}) \leq 2^{-n}$. Hence by Lemma (36), there is total recursive $g : N \to N$ such that $x \in \bigcap_n W_{g(n)}$, and for all n, $W_{g(n)}$ is prefix-free, and $\mathit{Pr}(W_{g(n)}) \leq 2^{-n}$. So:

(99) (a) for all $n \in N$, $W_{g(2n)}$ is prefix-free,
(b) $x \in \bigcap_n W_{g(2n)}$, and
(c) for all $n \in N$, $\mathit{Pr}(W_{g(2n)}) \leq 2^{-2n}$.

From (99)a,c via Lemma (69):

(100) $$\sum_{b \in W_{g(2n)}} 2^{-|b|} \leq 2^{-2n}.$$

We now show:

(101) $$\sum_{n \in N} \sum_{b \in W_{g(2n)}} 2^{n-|b|} \leq 1.$$

To demonstrate (101), observe that for all $n \in N$,

$$\sum_{b \in W_{g(2n)}} 2^{n-|b|} \;=\; \sum_{b \in W_{g(2n)}} 2^n 2^{-|b|} \;=\; 2^n \sum_{b \in W_{g(2n)}} 2^{-|b|} \;\leq\; 2^n 2^{-2n} \;=\; 2^{-n},$$

where the inequality follows from (100). Summing over n yields (101).

Returning to the proof of Proposition (98), let (n_i, b_i, ℓ_i) be a repetition-free, recursive enumeration of all triples with $n_i \in \mathbb{N}$, $b_i \in W_{g(2n_i)}$, and $\ell_i = |b_i| - n_i$. From (101) and the definition of ℓ_i we infer:

$$1 \geq \sum_{n \in N} \sum_{b \in W_{g(2n)}} 2^{n-|b|} = \sum_{n \in N} \sum_{b \in W_{g(2n)}} 2^{-(|b|-n)} = \sum_{i \in N} 2^{-\ell_i}.$$

Hence Lemma (38) implies that there is a recursive enumeration a_i of a prefix-free subset of B such that $|a_i| = \ell_i$ for all $i \in \mathbb{N}$. It follows from the two recursive enumerations that there is partial recursive function ψ with domain $\{a_i : i \in \mathbb{N}\}$ such that $\psi(a_i) = b_i$ for all $i \in \mathbb{N}$. Since $\{a_i : i \in \mathbb{N}\}$ is prefix-free, so is ψ. Thus we have:

> For all $n \in \mathbb{N}$ and $b \in W_{g(2n)}$ there is $i \in \mathbb{N}$ such that $|a_i| = |b| - n$ and $\psi(a_i) = b$.

It follows immediately that:

(102) For all $n \in \mathbb{N}$ and $b \in W_{g(2n)}$, $\mathcal{K}_\psi(b) \leq |b| - n$.

By Proposition (40), since ψ is prefix-free, choose c such that for all $b \in \mathsf{B}$, $\mathcal{K}(b) \leq \mathcal{K}_\psi(b) + c$. Then (102) implies:

> For all $n \in \mathbb{N}$ and $b \in W_{g(2n)}$, $\mathcal{K}(b) \leq \mathcal{K}_\psi(b) + c \leq |b| + c - n$.

Substituting for n in the foregoing, we obtain:

(103) For all $k \in \mathbb{N}$ and $b \in W_{g(2(c+k))}$, $\mathcal{K}(b) \leq |b| + c - (c + k) = |b| - k$.

In view of (99)b, for all $k \in \mathbb{N}$ there is $m \in \mathbb{N}$ such that $x[m] \in W_{g(2(c+k))}$. So (103) implies:

For all $k \in \mathbb{N}$ there is $m \in \mathbb{N}$ such that $\mathcal{K}(x[m]) \leq |x[m]| - k = m - k$.

By Definition (66), the last inequality shows x not to be KC-random. □

(104) COROLLARY: A real is ML-random if and only if it is CK-random.

From the preceding corollary and Corollary (93):

(105) COROLLARY: The set of reals that are random in the sense of Kolmogorov has probability 1.

References

BOOLOS, G. S., J. P. BURGESS, AND R. C. JEFFREY (2002): *Computability and Logic (4th Edition)*. Cambridge University Press, Cambridge UK.

DOWNEY, R., AND D. HIRSCHFELDT (2010): *Algorithmic Randomness and Complexity*. Springer.

LI, M., AND P. VITÁNYI (1997): *An introduction to Kolmogorov complexity and its applications (2nd Edition)*. Springer, New York NY.

OSHERSON, D., AND S. WEINSTEIN (2008): "Recognizing Strong Random Reals," *Review of Symbolic Logic*, 1(1), 56 – 63.

OXTOBY, J. C. (1971): *Measure and Category; A Survey of the Analogies between Topological and Measure Spaces*. Springer-Verlag, New York.

USPENSKII, V. A., A. L. SEMENOV, AND A. K. SHEN (1990): "Can an individual sequence of zeros and ones be random?," *Russian Mathematical Surveys*, 45.